COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas

Volume 2: Fall 2014

TABLE OF CONTENTS

Legal Risks of Wearable Technology

By John Browning

From smartwatches and fitbands that track your heart rate and other vital signs to Google Glass that enables wearers to record pictures and video with a simple voice command, wearable technology has arrived—and in a big way. This hot new field is currently generating an estimated $1.6 billion a year, and is expected to grow to $5 billion in revenue by 2016, according to a survey by Gartner. However, there can be a legal cost to wearing your heart (rate) on your sleeve. Wearable tech poses all kinds of legal risks, including data privacy, workplace privacy, and other legal issues.

Take Google Glass or other "smartglasses," for example. Designed to resemble a normal pair of glasses, the optical head-mounted display device takes the benefits of smartphone technology—mobility, connectivity, and assorted applications—and adds heightened engagement like enabling communications in the blink of an eye. Unlike a smartphone or camera that needs to be pointed, alerting third parties, Google Glass functions without the obvious telltale signs by the user. Conceivably, an employee could activate the device's recording feature with the press of a button or the blink of an eye and hover over someone's shoulder, recording login credentials, on-screen data, etc. As part of its social media features, Google Glass allows for the sharing of photos and videos via email or direct messaging. Imagine the information that could be surreptitiously gathered by an industrial spy, whistleblower, or an employee looking to assert employment claims: trade secrets and proprietary or confidential information, conversations in meetings, photos or video of employees. While Google, according to a spokesman, "built in explicit signals-including voice commands or gestures, along with the screen lighting up-to make it clear to others when someone is taking a picture or recording a video," many app developers have come up with nonconforming applications that circumvent Google policies. Such apps can be "sideloaded" on to a user's Glass device ("sideloading" refers to loading independently-developed apps onto the device by putting the device into test mode, not unlike "jailbreaking" an iPhone). Earlier this year, one developer designed a facial recognition app, NameTag, which enables Glass wearers to scan strangers' faces against known databases; this app is in direct contravention of Google's ban of facial recognition apps on Google Glass.

There are other legal risks as well. In October 2013, Google Glass wearer and software developer Cecilia Abadie was pulled over while driving on a San Diego highway, and was issued

a ticket for distracted driving under California Motor Vehicle Code Section 27602. The citation was later thrown out of court due to a lack of evidence that Abadie was distracted by, or even actually using, the device. While Abadie's case may have been the first Google Glass-related ticket, it won't be the last. Although more than 40 states have texting-while-driving laws on the books, most of these statutes exempt hands-free devices. But at least 8 states have introduced legislation that would ban the use of Google Glass while driving; these states are Delaware, Illinois, New York, New Jersey, West Virginia, Missouri, Maryland, and Wyoming. Yet once more, laws cannot hope to keep up with technology. According to William and Mary law professor Adam Gershowitz, author of a law review article proposing alternative legislative approaches to this issue, such bills would be practically unenforceable. "A driver could simply say that he was only wearing Google Glass (perhaps because it contains his prescription lenses) and that he was not 'using' the device at all," says Gershowitz. "Indeed, a police officer who was observing traffic would have no way to know whether a passing driver was 'using' as opposed to simply 'wearing' Google Glass," the professor writes. Where does Google itself stand in the issue? According to a Google spokesman, "Glass is built to connect you more with the world around you, not distract you from it. Glass wearers should always use Glass legally and responsibly and put their safety and the safety of others first."

Besides the potential for distracted driving liability, there are other legal risks as well with Google Glass. In January 2014 a moviegoer wearing Google Glass was removed from an AMC theater showing the movie "Jack Ryan: Shadow Recruit." In a scenario worthy of a Tom Clancy subplot itself, the movie patron was questioned for 2 hours by Homeland Security agents over potential film piracy changes. The man, who said he was wearing the device because it had his prescription lenses in it, was ultimately able to connect his Glass to a PC and demonstrate that he wasn't recording the movie. Around the U.S., establishments ranging from a restaurant in Seattle to strip clubs to casinos in Las Vegas have banned the use of smartglass technology. And for those users who too quickly give Glass the command to record, they could be exposing themselves to violations of state wiretapping laws—at least in the 12 states that require both parties to a conversation to consent to its recording (including Google's home state of California).

In addition to facing legal risks from third parties, users of wearable technology must contend with legal threats to themselves, particularly with regard to the privacy of their own data. Fitness tracking devices and health monitors like the Orbit fitness brand, Nike FuelBand, FitBit, or Jawbone, collect and analyze a dizzying array of physical activity metrics and biometric indicators. In some cases, these include pulse rate, blood sugar levels, blood pressure

readings, and other sensitive data. Even more sensitive than workout stats, wearable medical devices such as portable insulin pumps, can record and transmit information electronically to a website used by both patient and doctor. Such data may be subject to HIPAA restrictions and other privacy laws, meaning that wearable technology developers and users need to be concerned with the security of the data in the device as well as the security of data transmission. Wearable technology users would be well advised to study the privacy policy applicable to any device, in order to be aware of two main things—what specific kinds of data are being collected, and what is the company doing with that data? For example, who wouldn't want to know that the health tracker he received as a Father's Day present will be sharing his blood pressure readings with a health or life insurance carrier that may adjust their premiums accordingly? If a company that collects your data is going to share it with third parties, you should know about it and be able to respond accordingly, such as by opting out of the device's data-sharing functions. Wanting to lead a healthier lifestyle shouldn't be accompanied by sacrificing one's privacy.

Wearable tech can offer seemingly limitless benefits for the workplace, from smartglass recordings that can analyze workflow to improve efficiency and quality to wearable biometric sensors that can help prevent employee injuries and reduce the risks of workers' compensation claims. And employees seem open to the idea of wearable tech in the workplace. Santa Monica-based Cornerstone on Demand, which provides cloud-based talent management software solutions, released a "State of Workplace Productivity Report" in late 2013 that found that 58% of employees would be willing to use wearable tech if it enabled them to do their jobs better. However, employees need to be aware of the legal risks presented by wearable tech in the 21st century workplace. The recording capabilities of devices like Google Glass could compromise employee privacy or sensitive trade secrets. Recording footage of employees in restrooms or changing areas could lead to claims of a hostile work environment. And imagine the wrongful termination or retaliation lawsuit if an employee was terminated, only to have recorded Glass footage reveal that the employee had been discussing unionizing or other protected activity under the National Labor Relations Act. Just as with any technology in the workplace, companies would be well advised to address wearable tech in their BYOD ("Bring Your Own Device") policy, information security and/or internet usage policy, social media policy, etc. Technology use policies will need to include limitations on when recording functionality may be used, what the device may be used for, and when it should be inoperable. Biometric sensors and scanners can be particularly problematic, since they might reveal physical disabilities, illnesses, or protected physical conditions like pregnancy. Given the

protections offered by federal laws like the Americans with Disabilities Act or the Pregnancy Discrimination Act, employers might be put in the position of knowing certain things about an employee's physical condition and then being barred from taking any adverse employment action against that worker, as well as having to make reasonable accommodations for a newly discovered disability.

The wearable technology future has arrived, with all of its attendant benefits. But it also arrives with legal risks. As with any "disruptive" technology, courts and legislatures cannot hope to keep pace, but awareness of and planning for the legal issues presented by wearable technology can help mitigate risks and exposure. Those whose concerns about the invasiveness of this technology remain unabated may wish to reflect upon the furor among legal scholars like Louis Brandeis over a then-radical new device in 1890—the handheld camera. Society—and our legal system—adapted to new technology then, and they will continue to do so.

About the Author

John G. Browning is a partner in the Dallas office of Lewis Brisbois Bisgaard & Smith, where he practices a wide variety of civil litigation in state and federal courts. He is the author of three books and numerous articles on social media and the law, and he serves as an adjunct professor at SMU Dedman School of Law. Mr. Browning's work has been cited by courts across the country and in numerous law review articles, and publications like The New York Times, TIME magazine, Law 360, and others have quoted him as a leading expert on social media and the law.